

The Dyson Investigation

Appropriate Policy Document

This is the appropriate policy document for the Dyson Investigation ("the Investigation"). It sets out how the Investigation will protect personal information which falls within the definition of special category data or relates to criminal offences or allegations about criminal offences.

Special category data means personal information concerning an individual's racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; biometric data (used for identification purposes); physical or mental health; and sex life or sexual orientation.

Processing of special category data or data relating to criminal offences can only be carried out where certain safeguards are implemented. Paragraph 5 of Schedule 1 to the Data Protection Act 2018 applies where the processing is being carried out for reasons of substantial public interest. Paragraph 5 of Schedule 1 requires controllers to put an appropriate policy document in place in order to enable the processing of special category data or criminal offences data.

Purposes of data collection

Lord Dyson ("the Investigator") has been appointed by the BBC Board to carry out an independent investigation into the circumstances around the 1995 BBC Panorama Interview with Diana, Princess of Wales. The Investigator has appointed Fieldfisher LLP to act as Solicitors to the Investigation.

The purposes for which the Investigation collects and processes personal information are set out in the Terms of Reference.

The Investigation processes personal information for the purposes of its investigations and to enable it to carry out its work, including the conduct of interviews.

Personal information is used by the Investigation in a number of ways. Examples include:

- to seek evidence from potential witnesses through a call for evidence;
- to enable witnesses to give evidence about issues relevant to the terms of reference;
- to communicate with individuals involved in the Investigation;
- to provide the basis for the report.

Procedures for securing compliance

Article 5 of the United Kingdom General Data Protection Regulation sets out the data protection principles. These are the Investigation's procedures for ensuring that it complies with them.

Principle 1

Personal information shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

In order to comply with the first principle the Investigation will take the following steps:

- ensure that there is a legal basis for the processing of personal information and that processing is otherwise lawful;
- process personal information fairly in a way which individuals would expect, ensuring that they are not misled about the purposes of the processing; and
- enable transparency of processing, including providing a privacy notice on the Investigation's website.

Principle 2

Personal information shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

In order to comply with the second principle the Investigation will take the following steps:

- collect personal information for specified, explicit and legitimate purposes;
- inform data subjects about those purposes through the privacy notice; and
- not use personal information for purposes that are incompatible with the purposes for which it was collected.

Principle 3

Personal information shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

In order to comply with the third principle the Investigation will only collect, disclose or publish the minimum personal information that it needs for the purpose for which the information is processed. The Investigation will only seek to collect personal information which is relevant and adequate.

Principle 4

Personal information shall be accurate and, where necessary, kept up to date.

In order to comply with the fourth principle, the Investigation will ensure that personal information is accurate, and kept up to date where necessary.

Principle 5

Personal information shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal information is processed.

In order to comply with the fifth principle, the Investigation will only keep personal information in identifiable form until the conclusion of the Review. At the end of the Investigation the Investigator will produce a report. All personal information will be destroyed after any limitation period has expired in relation to the Investigation's work.

Principle 6

Personal information shall be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

In order to comply with the sixth principle, the Investigation will ensure that appropriate organisational and technical measures are in place to protect personal information. These may include only contracting with a secure third party database provider, password protecting sensitive documents before these are shared, and establishing a representations process before the Investigation is concluded and the report is finalised. The processes which the Investigation has put in place ensure that only personal information necessary for the performance of its functions will be disclosed outside the Investigation.

Accountability principle

The joint controllers shall be responsible for, and be able to demonstrate compliance with, these principles.

In order to comply with the accountability principle, the Investigation will:

- ensure that records are kept of all personal information processing activities;
- provide these to the Information Commissioner on request;
- carry out a Data Protection Impact Assessment for any high risk processing, and consult the Information Commissioner if appropriate; and
- have in place internal processes to ensure that personal information is only collected, used or handled in a way that is compliant with data protection law.

Policies as regards retention and erasure of personal information

The Investigation will ensure that where special category personal information or personal information relating to criminal offences is processed:

- there is a record of that processing and the record will set out, where possible, the envisaged time limits for erasure of the different categories of data;
- where it no longer requires special category data for the purpose for which it was collected, it will delete or anonymise the data; and
- data subjects receive (via the privacy notice) full privacy information about how their data will be handled, and that this will include the period for which the personal information will be stored, or if that is not possible, the criteria used to determine that period.

Further information

The Investigator and Fieldfisher LLP are joint controllers. Questions about this notice or processing by the Investigation can be directed to dyson@fieldfisher.com.